Common Criteria

The Cocktail Party Version

NISSC 98
7 October 1998

Tutorial Objectives

- Provide enough knowledge that you can sound like you know what you are talking about back at the office and at the next Security conference cocktail party
- Provide enough of an overview so you know what questions to ask
- Provide enough information that you know where to start

I want this tutorial to be

- Interactive
- Light
- Informative
- The kick-start you need to being a CC user and enthusiast

Questions to be answered

- What Is the CC?
- What Is the CC Not?
- Where did the CC come from?
- What are the central notions of the CC?
- What does the CC mean to me?
- What is the next step for the CC project?
- What do I do to get more information?

What is the CC?

- An internationally agreed framework for expressing IT security
- A means by which results of IT security evaluations can be recognized across boundaries
- An impending ISO standard (15408)
- Here !!!!!!

Other CC goals

- Mutual Recognition of evaluation results through harmonisation of existing security criteria
- Common Language and Understanding
- Flexibility in expressing security requirements
- Framework for criteria evolution

What the CC is Not

- THE answer to all the IT security questions and problems
- Simple
- Noncontroversial
- Universally adopted

- The new TCSEC

What - not replacing the TCSEC?

- The TCSEC was 5 sets of requirements decided by the DoD on what security functions their systems should have - security by mandate
- The CC provides tools for building reasonable sets of IT security requirements and for specifications of those requirements

More clarification

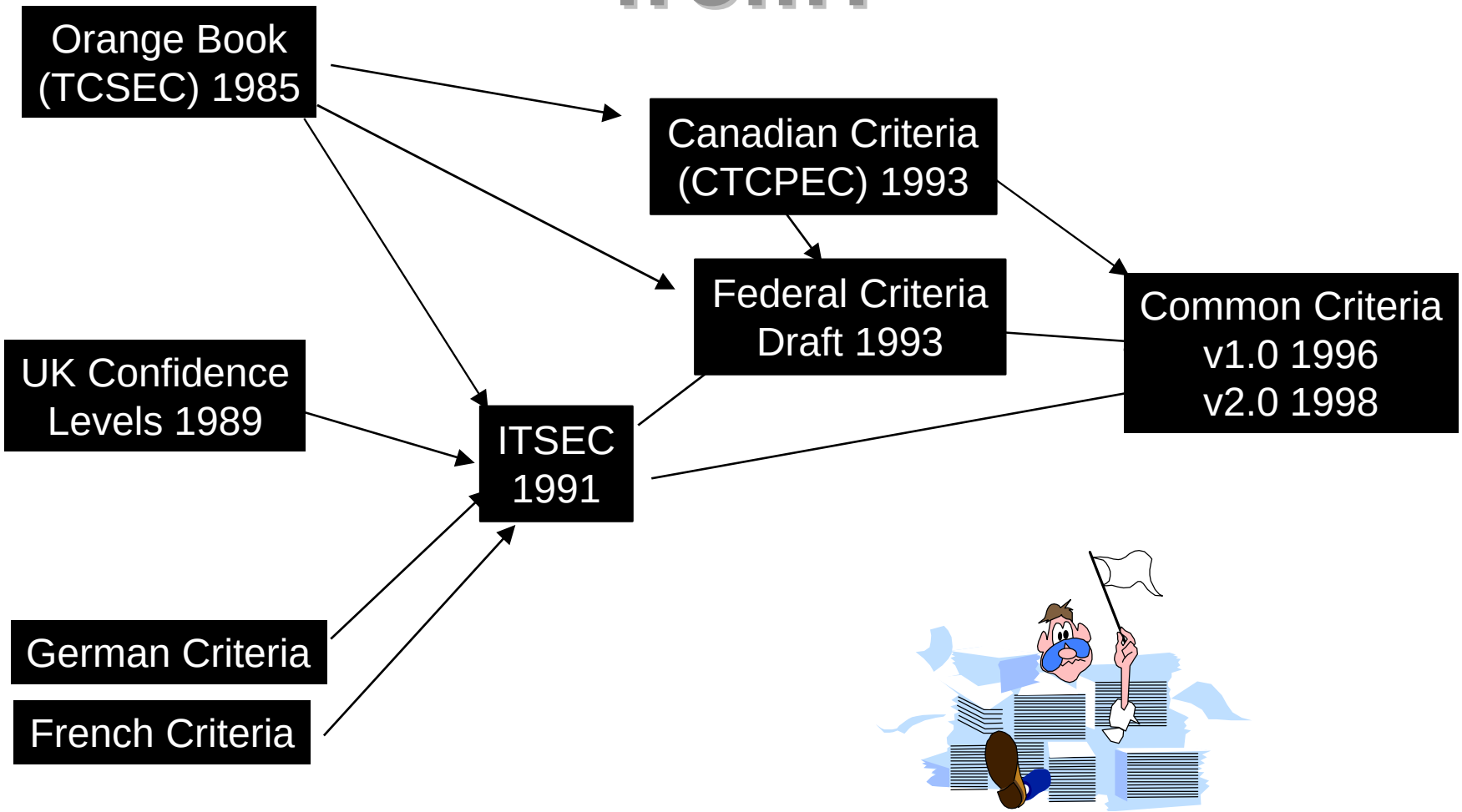
- TCSEC = newspaper article (or poem)
- CC = dictionary (or encyclopedia)

Still more - this is important

- The TCSEC ‘classes’ can be rebuilt from the CC encyclopedia
  (if you really want to)

- The CC gives you the building blocks to build the ‘classes’ that you really need

Where did the CC come from?



CC Sponsoring Agencies

- US-NSA
- US-NIST
- Canada-CSE
- France-SCSSI
- Germany-BSI
- Netherlands-NLNCSA
- United Kingdom-CESG

Other forces

- Security is not just for DoD anymore (Computer Security Act)
- Security is not just for Operating Systems anymore
- Security is about risk management not risk avoidance
- Need cost-effective solutions (no deep pockets)

More forces

- World market - one evaluation accepted by all (minimize cost)
- Need to compose systems from components
- Need to interoperate and have networked solutions

ISO involvement

- CC v2.0 in final committee draft
- Scheduled for (Final) Draft International Standard (FDIS) by end of October
- Scheduled for International Standard for May 1999

- Allows all to have input to the community criteria

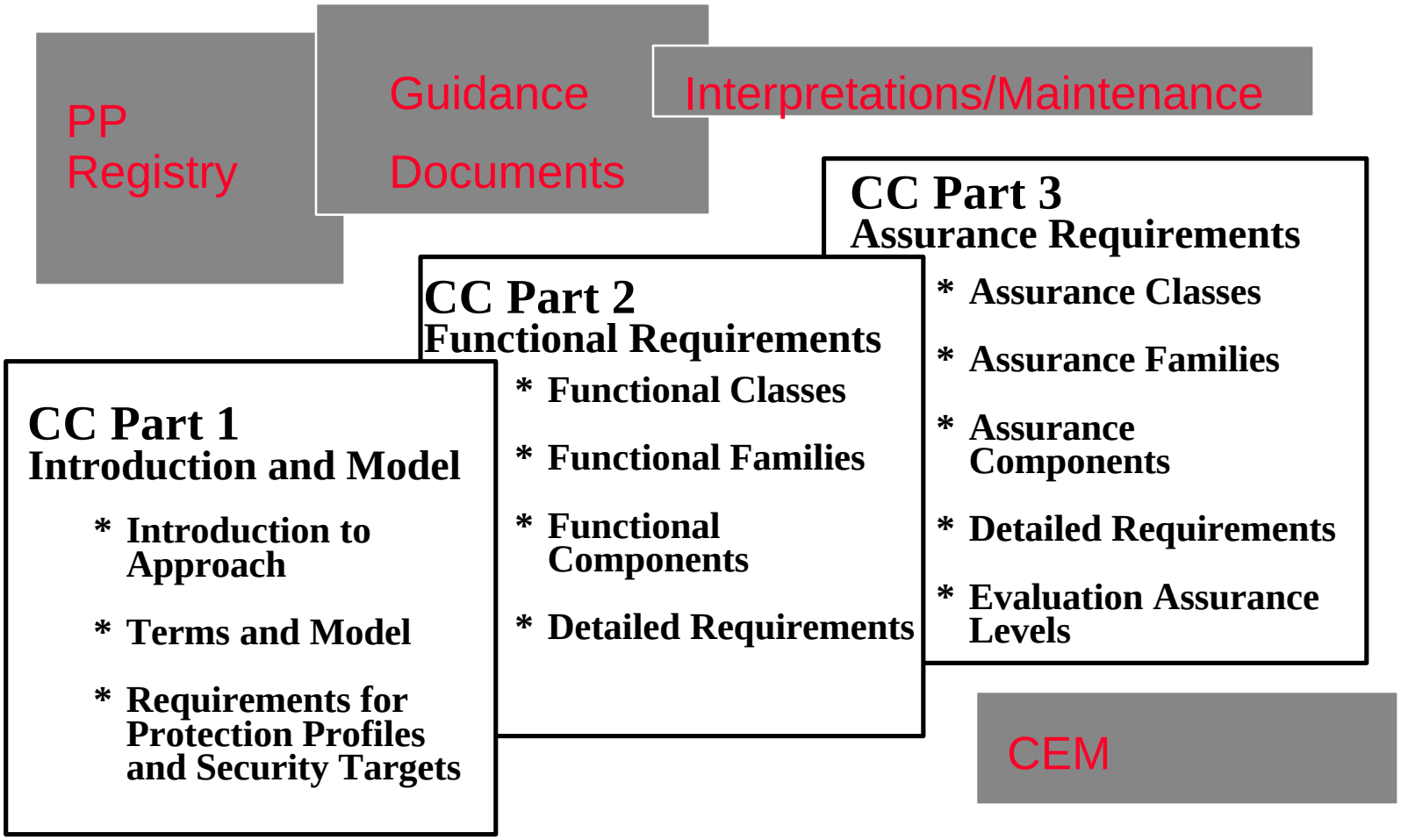
Other Sponsoring Organization Tasks

- Common Methodology
- Evaluation Schemes
- National interpretations
- National discussions
- Protection Profiles
- Maintain Evaluated Product Lists
- Other non-CC but IT Security information

Now for some Meat
CC Concepts

- Structure
  - Part 1 Introduction and General Model
  - Part 2 Security Functional Requirements
    - Requirements
    - Application Notes
  - Part 3 Security Assurance Requirements

CC Documentation



Key Concepts

- Component
- Protection Profile (PP)
- Security Target (ST)
- Package
- EAL
- Target of Evaluation (TOE)

Components

- CC has broken down traditional security into inseparable requirements (building blocks)
- Users can then compose their set of requirements
- Components can be refined to make more specific (close to specification)

Protection Profile

- Intended for expression of consumer needs
- Combination of security functional and security assurance requirements
- Allows for creation of security standards
- Assists backwards compatibility
- *Similar* to TCSEC classes

PP Contents

- Introduction
- TOE description
- Security environment
- Security objectives
- IT security requirements
- Application notes
- Rationale

Example PPs

- Role Based Access Control
- Application Gateway Firewall
- C2 equivalent
- DBMS (commercial)
- Electronic commerce, Smart card
- FIPS140-1
- Y2000

Security Target

- IT security objectives and requirements
- Functional and assurance measures
- Wide audience
- Suitable for products and systems
- *Similar* to ITSEC ST

ST Contents

- Similar to PP but add:
  - TOE summary specification
  - PP claims
  - Supporting rationale

Package

- IT security objectives and requirements
- Functions OR assurance (e.g. EAL)
- Wide audience, reusable
- Suitable for products and systems
- Similar to ITSEC E-levels

Functions vs. Assurance

- Function is something that the system does (behavior)
- Assurance is a means of generating confidence in those functions

Evaluation Assurance Levels

- Predefined Assurance Packages
- Agreed set of useful assurances

Target of Evaluation

- Whatever you are looking at
  - Product
  - System
  - Subsystem

What does all this mean?

- Mutual Recognition
  - Schemes recognize each others results
  - Vendors have bigger market with single evaluation
  - ‘Formal’ - always have choice to accept other results

What does this mean?

- New criteria means clean slate (?)
- You can influence the ‘standard’ sets of security specifications developed

Pros by Lynne

- It’s new
  - Learn from the past to move forward
- It’s flexible
  - You can define what you need - you are not limited to Big Brother telling you
- Everyone’s doing it
  - Community is involved and wants to use it

Cons by Lynne

- It’s new
  - Few people understand it, afraid of unknown...
- It’s flexible
  - Complex, have to think, easier to have someone else define
- Everyone’s doing it
  - Hard to keep track of what community is doing, conflicting ideas

Now what?

- Common Methodology for implementing the CC
- Maintain and extend the MR ‘arrangement’
- Add more sponsors
- Maintain and update CC
- Provide guidance and interpretations

What should you do next

- Participate in developing PPs
- Require CC in procurements
- Specify products in terms of CC STs
- Tell us what you think
- Spread the word

Where to get more info

- NIST Web Site
  - http://csrc.nist.gov/cc
- CC Support Environment
  - http://ccse.cesg.gov.uk
  - Initial prototype by 1 November
- me - lambuel@bdm.com 410-290-6041

Conclusion

- The CC is here - it is time to pay attention.
- It replaces the TCSEC but is something totally different
- Happy Day plus Ooooh Noooo.
- It’s not over - watch this space.